Barracuda Networks Predicts Spam Volumes Beyond 95 Percent in 2009

Submitted by: BondPR UK
Tuesday, 16 December 2008

Basingstoke, UK, 16th December, 2008 – Marking the five-year anniversary since the CAN-SPAM act was signed into law in the United States, Barracuda Networks Inc., the worldwide leader in email and Web security appliances, predicts that spam volumes will rise slightly higher than 95 percent in the year ahead as growing use of botnets continues to proliferate. An analysis of data from the more than one billion daily emails targeted at Barracuda Spam Firewalls worldwide, finds that spam levels in 2008 were largely unchanged over the previous year, making up between 90 and 95 percent of total email attempts.

“As the end of the year quickly approaches, many are asking if spam levels can get any worse in the new year,” said Stephen Pao, vice president of product management for Barracuda Networks. “There are a couple factors that we predict may cause spam to increase slightly in 2009, however, it is equally important to note that the level of legitimate email is also increasing each year.”

One such factor that may cause an increase in spam levels in the months to come is the emergence of spam originating from countries that had not previously been known for sending spam. For instance, Barracuda Central’s top 10 spam countries list ranks Brazil (6.77%) and Turkey (4.24%) in the second and fifth spots respectively.

“What is interesting is where both of these countries rank on the list relative to the 'usual suspects' of China (3.38%) and Russia (5.66%) in terms of spam originating countries,” said Pao. “We believe that this is due in part to both residential broadband penetration and proliferation of data centres in various countries around the world. As broadband availability increases, the reach and control of botnet activity also grows. Unsecured data centres are ripe for hacking and hosting of malicious content.”

Hidden identities to continue in 2009
Analysis of data from the more than one billion daily emails received by Barracuda Spam Firewalls found that identity obfuscation techniques were prevalent in a vast majority of spam campaigns sent in 2008. Hacked Web sites, the use of free hosting providers, as well as the rotation of new Web domains within the same campaign were all techniques that played major roles in hiding the identities of spammers in 2008.

“The investments that Barracuda Networks made in 2007 in the development of Predictive Sender Profiling techniques paid off big in 2008 as we successfully protected our customers from some of the most egregious spam attacks,” said Pao. “We believe that online scammers will continue to find news ways to hide their identities in 2009, making traditional IP reputation and content scanning less relevant.”

Predictive Sender Profiling capabilities provide industry-leading protection against spammers’ attempts to evade traditional reputation analysis. Utilizing a network of more than 70,000 customer systems worldwide, Barracuda Networks has the most diverse compilation of email available for profiling the behaviour of spammers. Using this data enables the Barracuda Spam Firewall to more easily fingerprint and block actual spam campaigns even when identity obfuscation techniques are used.

Increased reliance on brand names, social engineering techniques
In addition to botnet proliferation and identity obfuscation techniques, clever socially engineered phishing emails also continued to be a dominant force in 2008. In just the last quarter, several spam campaigns increased the use of trusted brands such as Microsoft and Google as well as more consumer-centric brands like Hallmark and McDonald's in attempts to lure recipients into providing personal account information, or as an attempt to persuade users to execute potentially malicious downloads onto their PCs.

"Phishing attacks are certainly not new techniques, but the levels of sophistication that are used can be quite astounding," said Pao.

"We believe that the combination of social engineering and sender identity obfuscation techniques will continue to merge, making it even more essential that customers use caution when accessing applications or providing personal information via URLs provided in emails," added Pao.

Barracuda Networks reminds email users to refrain from clicking on links within email from unknown or suspicious senders, and instead to copy and paste the link into their Web browser or visit the site directly.

About Barracuda Networks Inc.
Barracuda Networks Inc. isthe worldwide leader in email and Web security appliances. Barracuda Networks also provides world-class IM protection, application server load balancing, Web application security, message archiving, and backup and disaster recovery solutions. Coca-Cola, FedEx, Harvard University, IBM, L'Oreal, and Europcar, are amongst the 70,000 organizations protecting their networks with Barracuda Networks' solutions. Barracuda Networks' success is due to its ability to deliver easy to use, comprehensive solutions that solve the most serious issues facing customer networks without unnecessary add-ons, maintenance, lengthy installations or per user licence fees. Barracuda Networks is privately held with its headquarters in Campbell, California. Barracuda Networks has offices more than 10 international locations and distributors in more than 80 countries worldwide. For more information, please visit www.barracudanetworks.com.

# # #
For further press information please contact:
Paul Shlackman, BondPR
e: paul@bondpr.com
t: 01628 560 161